ref ?

141 — POLYNÔMES IRRÉDUCTIBLES À UNE INDÉTERMINÉE. CORPS DE RUPTURE. EXEMPLES ET APPLICATIONS.

Cadre : Soient A un anneau intègre et K un corps.

I - CRITÈRES D'IRRÉDUCTIBILITÉ

1) Définitions et premières propriétés

Déf 1 : Un polynôme $P \in A[X]$ est dit irréductible si c'est un élément irréductible de l'anneau $A[X]$, c'est-à-dire s'il est non nul non inversible et tel que

$$\forall P_1, P_2 \in A[X], \quad P = P_1 P_2 \implies P_1 \in A^\times \text{ ou } P_2 \in A^\times$$

Ex 2 : Tout polynôme de $K[X]$ de degré 1 est irréductible.

Prop 3 : Si $P \in K[X]$ est de degré 2 ou 3, alors P est irréductible ssi P n'a aucune racine dans K.

Ex 4 : . X^2+1 est irréductible dans $\mathbb{R}[X]$ (mais pas dans $\mathbb{C}[X]$).
. X^3-2 est irréductible dans $\mathbb{Q}[X]$ (mais pas dans $\mathbb{R}[X]$).

Cex 5 : $(2X+1)^2$ n'a pas de racine dans $\mathbb{Z}$, mais est réductible dans $\mathbb{Z}[X]$.

Prop 6 : Si K est algébriquement clos, les irréductibles de $K[X]$ sont exactement les polynômes de degré 1.

Cor 7 : . Les irréductibles de $\mathbb{C}[X]$ sont les polynômes de degré 1.
. Les irréductibles de $\mathbb{R}[X]$ sont les polynômes de degré 1 et les polynômes de degré 2 sans racine réelle.

Déf 8 : Supposons que A est factoriel. On dit que $P \in A[X] \setminus \{0\}$ est primitif si un pgcd de ses coefficients est 1.

Prop 9 : Supposons que A est factoriel et soit $K = \mathrm{Frac}(A)$. Les éléments irréductibles de $A[X]$ sont exactement :
- les éléments irréductibles de A ;
- les éléments de $A[X]$ non constants, primitifs et irréductibles dans $K[X]$.

Appli 10 : Si A est factoriel et $K = \mathrm{Frac}(A)$, alors $K[X]$ est factoriel.

Ex 11 : X^2-2 est primitif et irréductible dans $\mathbb{Q}[X]$, donc irréductible dans $\mathbb{Z}[X]$.

Cex 12 : $2X$ est irréductible dans $\mathbb{Q}[X]$, mais pas dans $\mathbb{Z}[X]$.

2) Quelques autres critères d'irréductibilité

Th 13 : (Critère d'Eisenstein)
Supposons que A est factoriel et soit $K = \mathrm{Frac}(A)$.
Soient $P = a_nX^n + \dots + a_1X + a_0 \in A[X]$ et $p \in A$ irréductible tels que $p \nmid a_n$, $p^2 \nmid a_0$ et $\forall i \in [\![0, n-1]\!]$, $p \mid a_i$.
Alors P est irréductible dans $K[X]$.

Ex 14 : . $3X^4 + 15X^2 + 10$ est irréductible dans $\mathbb{Q}[X]$ et $\mathbb{Z}[X]$.
. Si p est premier, $X^{p-1} + \dots + X + 1$ est irréductible dans $\mathbb{Q}[X]$ et $\mathbb{Z}[X]$.

Th 15 : (Critère de réduction modulo un idéal premier)
Supposons que A est factoriel et soit $K = \mathrm{Frac}(A)$.
Soient I un idéal premier de A, $B = A/I$ et $L = \mathrm{Frac}(B)$.
Soient $P = a_nX^n + \dots + a_1X + a_0 \in A[X]$ et $\overline{P}$ sa réduction modulo I.
Si $\overline{a_n} \neq 0$ et si $\overline{P}$ est irréductible dans $B[X]$ ou $L[X]$, alors P est irréductible dans $K[X]$.

Ex 16 : $X^3 + 462X^2 + 2433X - 67691$ est irréductible dans $\mathbb{Q}[X]$ et $\mathbb{Z}[X]$.

Cex 17 : X^2-2 est irréductible dans $\mathbb{Q}[X]$, mais pas dans $\frac{\mathbb{Z}}{2\mathbb{Z}}[X]$.

Prop 18 : Si $P = a_nX^n + \dots + a_1X + a_0 \in \mathbb{C}[X]$ avec $a_n \neq 0$, alors pour toute racine $\alpha \in \mathbb{C}$ de P :

$$|\alpha| \leq \max\left\{1 ; \sum_{i=0}^{n-1} \frac{|a_i|}{|a_n|}\right\}.$$

Prop 19 : Soit $P = a_nX^n + \dots + a_1X + a_0 \in \mathbb{Z}[X]$.
S'il existe $x \in \mathbb{Z}$ tel que $|x| > \max\limits_{i \in [\![0,n]\!]} |a_i| + 1$ et $|P(x)|$ est premier ou égal à 1, alors P est irréductible dans $\mathbb{Z}[X]$.

Ex 20 : Les racines de $P = 5X^4 + 2X^3 - 3X^2 + 7X + 8$ sont contenues dans $D(0,4)$ et $P(7) = 12601$ est premier, donc P est irréductible dans $\mathbb{Z}[X]$.

Th21 : (Critère d'Ore)
Soient $P \in \mathbb{Z}[X]$ de degré $n \geq 1$ et $a_1, \dots, a_{n+5}$ $n+5$ entiers distincts tels que $\forall i \in [\![1, n+5]\!]$, $|P(a_i)|$ est premier ou égal à 1.
Alors P est irréductible dans $\mathbb{Q}[X]$.

Appli22 : $P = X^4 - 72X^2 + 4$ est irréductible dans $\mathbb{Q}[X]$, car $|P(a_i)|$ est premier si $a_i \in \{\pm 1; \pm 3; \pm 5; \pm 7; \pm 9\}$.

Rem23 : Il suffit en fait de vérifier le critère d'Ore pour $n+3$ entiers. (ADMIS)

II - ADJONCTION DE RACINES

1) Éléments algébriques, extensions algébriques

Soit L/K une extension de corps.

Prop-Déf24 : Soient $x \in L$ et $\varphi_x : K[X] \to L$ l'unique morphisme de K-algèbres tel que $\varphi_x(X) = x$.
- Si φ_x est injectif, on dit que x est transcendant sur K.
- Sinon, on dit que x est algébrique sur K, et dans ce cas, il existe un unique polynôme unitaire $\pi_{x,K}$ tel que $\mathrm{Ker}(\varphi_x) = (\pi_{x,K})$. $\pi_{x,K}$ est appelé le polynôme minimal de x sur K, et il est irréductible dans $K[X]$.

Ex25 : $\sqrt[3]{2}$ est algébrique sur $\mathbb{Q}$ et $\pi_{\sqrt[3]{2},\mathbb{Q}} = X^3 - 2$.

Prop26 : Soit $x \in L$.
- Si x est algébrique sur K, alors $\frac{K[X]}{(\pi_{x,K})} \overset{K\text{-alg}}{\cong} K[x] = K(x)$.
  De plus $(1, x, \dots, x^{\deg(\pi_{x,K})-1})$ forme une base de $K(x)$ sur K.
- Si x est transcendant sur K, alors $K[X] \overset{K\text{-alg}}{\cong} K[x]$ et $K(X) \overset{K\text{-alg}}{\cong} K(x)$.

Déf27 : On dit que L/K est une extension algébrique si tout élément de L est algébrique sur K.

Prop28 : Si L/K est finie, alors elle est algébrique, de type fini et pour tout $x \in L$, $\deg(\pi_{x,K}) \leq [L:K]$.

Th29 : Si $L = K(x_1, \dots, x_n)$ où x_i est algébrique sur K, alors $L = K[x_1, \dots, x_n]$, L/K est algébrique et finie, avec
$$[L:K] \leq \prod_{i=1}^{n} \deg(\pi_{x_i,K})$$

Cor30 : L/K est finie ssi L/K est algébrique et de type fini.

Appli31 : $L_{alg/K} = \{x \in L \mid x \text{ est algébrique sur } K\}$ est un sous-corps de L, appelé la fermeture algébrique de K dans L.

Ex32 : L'ensemble $\overline{\mathbb{Q}}$ des éléments algébriques sur $\mathbb{Q}$ est un sous-corps de $\mathbb{C}$.

2) Corps de rupture, corps de décomposition

Déf33 : Soient L/K une extension de corps et $P \in K[X]$ irréductible. On dit que L est un corps de rupture de P sur K si $L = K(x)$ et $P(x) = 0$.

Ex34 : $X^3 - 2$ est irréductible sur $\mathbb{Q}$ et $\mathbb{Q}(\sqrt[3]{2})$, $\mathbb{Q}(j\sqrt[3]{2})$ et $\mathbb{Q}(j^2 \cdot \sqrt[3]{2})$ sont des corps de rupture de P sur $\mathbb{Q}$.

Thm35 : Soient K un corps et $P \in K[X]$ irréductible. Il existe un corps de rupture de P sur K, unique à isomorphisme près.

Appli36 : Soient K un corps et $P \in K(X)$ tel que $\deg P = n \geq 1$. P est irréductible dans $K[X]$ ssi P n'a pas de racine dans les extensions L de K telles que $[L:K] \leq n/2$.

Déf37 : Soient L/K une extension de corps et $P \in K[X]$ de degré $n \geq 1$. On dit que L est un corps de décomposition de P sur K si P est scindé dans $K[X]$ et L est engendré sur K par les racines de P.

Ex38 : $\mathbb{Q}(\sqrt[3]{2}, j)$ est un corps de décomposition de X^3-2 sur $\mathbb{Q}$.

Th39 : Soient K un corps et $P \in K(X)$ de degré $n \geq 1$.
Il existe un corps de décomposition de P sur K, unique à isomorphisme près. De plus si L est un corps de décomposition de P sur K, alors $[L:K] \leq n!$.

Ex40 : $\mathbb{C}$ est à la fois corps de rupture et de décomposition de X^2+1 sur $\mathbb{R}$.

Appli41 : Existence et unicité des corps finis.

Thm42 : (Théorème de l'élément primitif)
Soient K un corps tel que $car(K)=0$ et L/K une extension finie.
Il existe $x \in L$ tel que $L = K(x)$.

Déf43 : Soit L/K une extension de corps.
On dit que L est une clôture algébrique de K si L est algébriquement clos et tout élément de L est algébrique sur K.

Th44 : $\overline{\mathbb{Q}}$ est une clôture algébrique de $\mathbb{Q}$.

Th45 : (Théorème de Steinitz) [ADMIS]
Tout corps K possède une clôture algébrique, unique à K-isomorphisme près.

III - POLYNÔMES IRRÉDUCTIBLES SUR LES CORPS FINIS

Soient p un nombre premier, $r \geq 1$ et $q = p^r$.

1) Dénombrement des polynômes irréductibles sur $\mathbb{F}_q$

On note $I(n,q)$ l'ensemble des polynômes irréductibles unitaires de degré n sur $\mathbb{F}_q$ et $m(n,q) = |I(n,q)|$.

DVPT ①

Prop46 : $\forall n \geq 1$, $X^{q^n} - X = \prod_{d|n} \prod_{P \in I(d,q)} P$

Déf47 : On appelle fonction de Möbius la fonction $\mu : \mathbb{N}^* \to \{-1,0,1\}$ définie par $\mu(1)=1$ et $\forall n \geq 2$, $\mu(n) = \begin{cases} 0 & \text{si } n \text{ a un facteur carré} \\ (-1)^r & \text{si } n = p_1 \cdots p_r \text{ avec les } p_i \text{ premiers distincts} \end{cases}$

Prop48 :
- $\forall n \geq 1$, $I(n,q) = \frac{1}{n} \sum_{d|n} \mu\left(\frac{n}{d}\right) q^d$
- $I(n,q) \underset{n \to \infty}{\sim} \frac{q^n}{n}$

Appli49 : (Test de Rabin)
Soit $P \in \mathbb{F}_q[X]$ de degré $n \geq 1$.
P est irréductible dans $\mathbb{F}_q[X]$ ssi P divise $X^{q^n} - X$ et pour tout diviseur premier s de n, $P \wedge (X^{q^{n/s}} - X) = 1$.

2) Algorithme de Berlekamp

Algo50 : (Algorithme de factorisation)
Soit $P \in \mathbb{F}_q[X]$ non constant.
- Si $P' = 0$, alors il existe $R \in \mathbb{F}_q[X]$ tel que $P = R^p$. On réapplique l'algorithme à R.
- Si $P' \neq 0$ et $D = P \wedge P' \neq 1$, on réapplique l'algorithme à D et $\frac{P}{D}$.
- Si $P' \neq 0$ et $D = P \wedge P' = 1$, alors P est sans facteur carré et on arrête.

On a ainsi décomposé P en produit de polynômes sans facteur carré.

DVPT ②

Algo51 : (Algorithme de Berlekamp)
Soient $P \in \mathbb{F}_q[X]$ non constant et sans facteur carré, et x la classe de X dans $\mathbb{F}_q[X]/(P)$.
On note $\varphi_P : \begin{array}{ccc} \mathbb{F}_q[X]/(P) & \longrightarrow & \mathbb{F}_q[X]/(P) \\ Q & \longmapsto & Q^q \end{array}$ qui est $\mathbb{F}_q$-linéaire.

- On calcule la matrice de $\varphi_P - id$ dans la base $(1, x, \dots, x^{\deg P - 1})$ et son noyau.
- Si $\dim \mathrm{Ker}(\varphi_P - id) = 1$, alors P est irréductible et on arrête.
Sinon on calcule un polynôme Q non constant modulo P et tel que $Q \bmod P \in \mathrm{Ker}(\varphi_P - id)$.
Alors $P = \prod_{\alpha \in \mathbb{F}_q} P \wedge (Q - \alpha)$ et tous les facteurs non constants sont non triviaux, et on réapplique l'algorithme à ces facteurs non triviaux.